/[redacted]/ - /[redacted]/

Real News Without Shills or Trolls

Catalog

Posting mode: Reply [Return] [Go to bottom]

Name	
Email	
Subject	New Reply
Comment *	
File	Choose File No file selected

* = required field

[Show post options & limits]

Confused? See the FAQ.

File: 4cf3261987a2589[redacted].png (235.67 KB, 400x400, 1:1, C6UVIISWUAEsNla.png)

WikiLeaks Publishes Huge Trove of CIA Spying Documents Anonymous 03/07/17 (Tue) 15:13:57 No.2003

WikiLeaks has published a huge trove of what appear to be CIA spying secrets.

http://archive.is/2Gf6s
https://twitter.com/wikileaks/status/838910359994056704
http://archive.is/W2s0x
https://twitter.com/wikileaks/status/839100031256920064

The files are the most comprehensive release of US spying files ever made public, according to Julian Assange. In all, there are 8,761 documents that account for "the entire hacking capacity of the CIA", Mr Assange claimed in a release, and the trove is just the first of a series of "Vault 7" leaks.

Already, the files include far more pages than the Snowden files that exposed the vast hacking power of the NSA and other agencies.

In publishing the documents, WikiLeaks had ensured that the CIA had "lost control of its arsenal", he claimed. That included a range of software and exploits that if real could allow unparalleled control of computers around the world.

It includes software that could allow people to take control of the most popular consumer electronics products used today, claimed WikiLeaks.

"'Year Zero' introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones," the organisation said in a release.

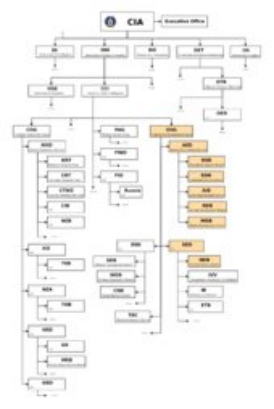
The files were made available by a source who intended them to start a conversation about whether the CIA had gained too much power, according to the organisation.

"In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency," a release read. "The source wishes to initiate a

public debate about the security, creation, use, proliferation and democratic control of cyberweapons."

http://archive.is/4PuII
http://www.independent.co.uk/life-style/gadgets-and-tech/news/wikileaks-cia-vault-7-julian-assange-year-zero-documents-download-spying-secrets-a7616031.html

Wikileaks Unveils The Largest Ever Publication Of Confidential CIA Documents **Anonymous** 03/07/17 (Tue) 15:14:40 No.2004
File: 3c0cc31e4f2a153□.png (289.88 KB, 1800x2700, 2:3, Chart-CIA-Year0.png)



WikiLeaks has published what it claims is the largest ever release of confidential documents on the CIA. It includes more than 8,000 documents as part of 'Vault 7', a series of leaks on the agency, which have allegedly emerged from the CIA's Center For Cyber Intelligence in Langley, and which can be seen on the org chart, which Wikileaks also released.

A total of 8,761 documents have been published as part of 'Year Zero', the first in a series of leaks the whistleblower organization has dubbed 'Vault 7.' WikiLeaks said that 'Year Zero' revealed details of the CIA's "global covert hacking program," including "weaponized exploits" used against company products including "Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones."

WikiLeaks tweeted the leak, which it claims came from a network inside the CIA's Center for Cyber Intelligence in Langley, Virginia.

But perhaps what is most notable is the purported emergence of another Snowden-type whistleblower: the source of the information told WikiLeaks in a statement that they wish to initiate a public debate about the "security, creation, use, proliferation and democratic control of cyberweapons." Policy questions that should be debated in public include "whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency," WikiLeaks claims the source said.

The FAQ section of the release, shown below, provides further details on the extent of the leak, which was "obtained recently and covers through 2016". The time period covered in the latest leak is between the years 2013 and 2016, according to the CIA timestamps on the documents themselves. Secondly, WikiLeaks has asserted that it has not mined the entire leak and has only verified it, asking that journalists and activists do the leg work.

Among the various techniques profiled by WikiLeaks is "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As Kim Dotcom chimed in on Twitter, "CIA turns Smart TVs, iPhones, gaming consoles and many other consumer gadgets into open microphones" and added " CIA turned every Microsoft Windows PC in the world into spyware. Can activate backdoors on demand, including via Windows update"

>BREAKING: CIA turns Smart TVs, iPhones, gaming consoles and many other consumer gadgets into open microphones. #Vault7

— Kim Dotcom (@KimDotcom) March 7, 2017

Dotcom also added that "Obama accused Russia of cyberattacks while his CIA turned all internet enabled consumer electronics in Russia into listening devices. Wow!"

>Obama accused Russia of cyberattacks while his CIA turned all internet enabled consumer electronics in Russia into listening devices. Wow!

— Kim Dotcom (@KimDotcom) March 7, 2017

http://archive.is/AFfS2
http://www.zerohedge.com/news/2017-03-07/wikileaks-hold-press-conference-vault-7-release-8am-eastern

MI5 and CIA Targeted iPhones, Microsoft and Samsung TVs For Global Hacking Program **Anonymous** 03/07/17 (Tue) 15:15:13 No.2005
File: 63cabea8e3f8780□.jpg (106.8 KB, 1158x496, 579:248, C6UI_W2WYAALaLv.jpg)


The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.

The attack against Samsung smart TVs was developed in cooperation with the United Kingdom's MI5/BTSS. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks. The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations.

WikiLeaks has claimed the CIA targeted iPhones and Microsoft Windows and worked with MI5 to turn Samsung TVs into microphones as part of a global hacking programme.

The secretive organisation is about to release a huge trove of confidential documents from the U.S. Central Intelligence Agency as part of its mysterious Year Zero series, founder Julian Assange claimed.

It has issued the release amid claims the CIA has been carrying out a global covert hacking program that exploits US and European company products.

It claims these include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which it says "are turned into covert microphones."

In an online statement on its website, Wikileaks also claims the attack against Samsung smart TVs was developed in cooperation with the UK's domestic intelligence agency MI5/BTSS.

It states: "After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on.

"In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the internet to a covert CIA server."

Mr Assange said: "There is an extreme proliferation risk in the development of cyber 'weapons'.

"Comparisons can be drawn between the uncontrolled proliferation of such 'weapons', which results from the inability to contain them combined with their high market value, and the global arms trade.

"But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace.

"The disclosure is also exceptional from a political, legal and forensic perspective."

The hacking group said the publication release is from 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence.

Wikileaks said: "Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation.

http://archive.is/KR5M3
http://www.mirror.co.uk/news/world-news/year-zero-series-wikileaks-cia-9981832

Anonymous 03/07/17 (Tue) 15:52:14 No.2006

Vault 7: CIA Hacking Tools Revealed

http://archive.is/Kc6H9
https://wikileaks.org/ciav7p1/

Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina. It follows an introductory disclosure last month of CIA targeting French political parties and candidates in the lead up to the 2012 presidential election.

Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

"Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.

Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force — its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.

By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (CCI), had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified.

In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.

Once a single cyber 'weapon' is 'loose' it can spread around the world in seconds, to be used by rival states, cyber mafia and teenage hackers alike.

Julian Assange, WikiLeaks editor stated that "There is an extreme proliferation risk in the development of cyber 'weapons'. Comparisons can be drawn between the uncontrolled proliferation of such 'weapons', which results from the inability to contain them combined with their high market value, and the global arms trade. But the significance of "Year Zero" goes well beyond the choice between cyberwar and cyberpeace. The disclosure is also exceptional from a political, legal and forensic perspective."

Wikileaks has carefully reviewed the "Year Zero" disclosure and published substantive CIA documentation while avoiding the distribution of 'armed' cyberweapons until a consensus emerges on the technical and political nature of the CIA's program and how such 'weapons' should analyzed, disarmed and published.

Wikileaks has also decided to redact and anonymise some identifying information in "Year Zero" for in depth analysis. These redactions include ten of thousands of CIA targets and attack machines throughout Latin America, Europe and the United States. While we are aware of the imperfect results of any approach chosen, we remain committed to our publishing model and note that the quantity of published pages in "Vault 7" part one ("Year Zero") already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks.

Anonymous 03/07/17 (Tue) 15:52:41 No.2007

CIA malware targets iPhone, Android, smart TVs

http://archive.is/Kc6H9#selection-1257.0-1257.46

CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA (see this organizational chart of the CIA for more details).

The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide.

The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's Embedded Devices Branch (EDB), which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.

The attack against Samsung smart TVs was developed in cooperation with the United Kingdom's MI5/BTSS. After infestation, Weeping Angel places the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks. The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations.

The CIA's Mobile Devices Branch (MDB) developed numerous attacks to remotely hack and control popular smart phones. Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone.

Despite iPhone's minority share (14.5%) of the global smart phone market in 2016, a specialized unit in the CIA's Mobile Development Branch produces malware to infest, control and exfiltrate data from iPhones and other Apple products running iOS, such as iPads. CIA's arsenal includes numerous local and remote "zero days" developed by CIA or obtained from GCHQ, NSA, FBI or purchased from cyber arms contractors such as Baitshop. The disproportionate focus on iOS may be explained by the popularity of the iPhone among social, political, diplomatic and business elites.

A similar unit targets Google's Android which is used to run the majority of the world's smart phones (~85%) including Samsung, HTC and Sony. 1.15 billion Android powered phones were sold last year. "Year Zero" shows that as of 2016 the CIA had 24 "weaponized" Android "zero days" which it has developed itself and obtained from GCHQ, NSA and cyber arms contractors.

These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is applied.

Anonymous 03/07/17 (Tue) 15:52:54 No.2008

CIA malware targets Windows, OSx, Linux, routers

http://archive.is/Kc6H9#selection-1377.0-1377.48

The CIA also runs a very substantial effort to infect and control Microsoft Windows users with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" which infects software distributed on CD/DVDs, infectors for removable media such as USBs, systems to hide data in images or in covert disk areas ("Brutal Kangaroo") and to keep its malware infestations going.

Many of these infection efforts are pulled together by the CIA's Automated Implant Branch (AIB), which has developed several attack systems for automated infestation and control of CIA malware, such as "Assassin" and "Medusa".

Attacks against Internet infrastructure and webservers are developed by the CIA's Network Devices Branch (NDB).

The CIA has developed automated multi-platform malware attack and control systems covering Windows, Mac OS X, Solaris, Linux and more, such as EDB's "HIVE" and the related "Cutthroat" and "Swindle" tools, which are described in the examples section below.

Anonymous 03/07/17 (Tue) 15:53:08 No.2009

CIA 'hoarded' vulnerabilities ("zero days")

http://archive.is/Kc6H9#selection-1467.0-1467.43

In the wake of Edward Snowden's leaks about the NSA, the U.S. technology industry secured a commitment from the Obama administration that the executive would disclose on an ongoing basis — rather than hoard — serious vulnerabilities, exploits, bugs or "zero days" to Apple, Google, Microsoft, and other US-based manufacturers.

Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others.

The U.S. government's commitment to the Vulnerabilities Equities Process came after significant lobbying by US technology companies, who risk losing their share of the global market over real and perceived hidden vulnerabilities. The government stated that it would disclose all pervasive vulnerabilities discovered after 2010 on an ongoing basis.

"Year Zero" documents show that the CIA breached the Obama administration's commitments. Many of the vulnerabilities used in the CIA's cyber arsenal are pervasive and some may already have been found by rival intelligence agencies or cyber criminals.

As an example, specific CIA malware revealed in "Year Zero" is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter accounts. The CIA attacks this software by using undisclosed security vulnerabilities ("zero days") possessed by the CIA but if the CIA can hack these phones then so can everyone else who has obtained or discovered the vulnerability. As long as the CIA keeps these vulnerabilities concealed from Apple and Google (who make the phones) they will not be fixed, and the phones will remain hackable.

The same vulnerabilities exist for the population at large, including the U.S. Cabinet, Congress, top CEOs, system administrators, security officers and engineers. By hiding these security flaws from manufacturers like Apple and Google the CIA ensures that it can hack everyone &mdsh; at the expense of leaving everyone hackable.

Anonymous 03/07/17 (Tue) 15:53:29 No.2010

Evading forensics and anti-virus

http://archive.is/Kc6H9#selection-1747.0-1747.32

A series of standards lay out CIA malware infestation patterns which are likely to assist forensic crime scene investigators as well as Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens and anti-virus companies attribute and defend against attacks.

"Tradecraft DO's and DONTs" contains CIA rules on how its malware should be written to avoid fingerprints implicating the "CIA, US government, or its witting partner companies" in "forensic review". Similar secret standards cover the use of encryption to hide CIA hacker and malware communication (pdf), describing targets & exfiltrated data (pdf) as well as executing payloads (pdf) and persisting (pdf) in the target's machines over time.

CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in AV defeats, Personal Security Products, Detecting and defeating PSPs and PSP/Debugger/RE Avoidance. For example, Comodo was defeated by CIA malware placing itself in the Window's "Recycle Bin". While Comodo 6.x has a "Gaping Hole of DOOM".

CIA hackers discussed what the NSA's "Equation Group" hackers did wrong and how the CIA's malware makers could avoid similar exposure.

Examples

http://archive.is/Kc6H9#selection-1859.0-1859.8

The CIA's Engineering Development Group (EDG) management system contains around 500 different projects (only some of which are documented by "Year Zero") each with their own sub-projects, malware and hacker tools.

The majority of these projects relate to tools that are used for penetration, infestation ("implanting"), control, and exfiltration.

Another branch of development focuses on the development and operation of Listening Posts (LP) and Command and Control (C2) systems used to communicate with and control CIA implants; special projects are used to target specific hardware from routers to smart TVs.

Some example projects are described below, but see the table of contents for the full list of projects described by WikiLeaks' "Year Zero".

http://archive.is/Kc6H9

Wikileaked! CIA Able to Access Encrypted Data on Telegram, WhatsApp Anonymous 03/07/17 (Tue) 16:09:38 No.2011
File: 81edc0b54ed44ff□.jpg (32.75 KB, 615x358, 615:358, C6Ucgf7WcAEy5Ou.jpg)

Wikileaked! CIA Able to Access Encrypted Data on Telegram, WhatsApp

The US Central Intelligence Agency (CIA) can hack smartphones and access encrypted information from Telegram, WhatsApp, Signal and Wiebo messengers, the whistleblowing website WikiLeaks said Tuesday, citing confidential information leaked from the CIA.

According to the organization, the CIA has several units specializing in malware designed for specific smartphone operating systems, with dedicated branches for Apple's iOS and Google's Android.

"These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the 'smart' phones that they run on and collecting audio and message traffic before encryption is applied," the WikiLeaks press release said.

The CIA reportedly failed to disclose serious vulnerabilities, also known as "zero days," of various technology products and proceeded to use them to target the relevant software.

Earlier on Tuesday, the WikiLeaks began to release what it said was an unprecedentedly large archive of CIA-related classified documents.

The first part of the leaks dubbed "Year Zero" comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virgina.

"The quantity of published pages in "Vault 7" part one ("Year Zero") already eclipses the total number of pages published over the first three years of the Edward Snowden NSA leaks."

http://archive.is/qMdqL
https://sputniknews.com/world/201703071051348537-cia-wikileaks-telegram-whatsapp/

CIA Plans to Hack Cars and Trucks to Carry Out Undetectable Assassinations Anonymous 03/07/17 (Tue) 16:49:00 No.2013
File: e0e966cc1adc8b0□.jpg (158.83 KB, 728x380, 182:95, car-hacking-jeep.jpg)

WikiLeaks has claimed the CIA planned to hack cars and trucks to carry out assassinations.

The secretive organisation said the U.S. Central Intelligence Agency used the phone's geolocation software to tap into vehicle control systems in modern cars.

The hacking organisation made the statement as it announced a huge release of confidential documents from the CIA as part of its mysterious Year Zero series, founder Julian Assange claimed.

It claims the CIA has been carrying out a global covert hacking program that exploits US and European companies.

It claims these include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which it says "are turned into covert microphones."

Mr Assange was set to speak about Year Zero on Facebook today, but a livestream of the event was reportedly hacked. It is not clear when the event has been rescheduled to.

The group said that from October 2014 the CIA was "looking at infecting the vehicle control systems used by modern cars and trucks" to possibly enable them to "engage in nearly undetectable assassinations."

They added: "The CIA's Mobile Devices Branch (MDB) developed numerous attacks to remotely hack and control popular smart phones."

They claimed these included iPhones, which account for 14% of the market and Google Android, "which is used to run the majority of the world's smart phones (85%) including Samsung, HTC and Sony. 1.15 billion Android powered phones were sold last year."

They claimed: "Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone."

http://archive.is/kqWXj
http://www.mirror.co.uk/news/world-news/year-zero-series-wikileaks-cia-9982483

[Return] [Go to top] [Catalog]

NEWS PLUS

Breaking news! (+)

President Trump Praises ExxonMobil As White House Echoes Exxon Press Release

by: Printz ## Reporter